#3

PATENT
81942.0004
Express Mail Label No. EL 589 806 385 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Kiyoshi OGISHI et al.

Serial No: Not assigned

Filed: November 7, 2000

For: KEY SHARING METHOD, SECRET KEY GENERATING METHOD, COMMON KEY GENERATING METHOD AND CRYPTOGRAPHIC COMMUNICATION METHOD IN ID-NIKS CRYPTOSYSTEM

Art Unit: Not assigned

Examiner: Not assigned

TRANSMITTAL OF PRIORITY DOCUMENT

Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed herewith is a certified copy of Japanese patent application No. 2000-133471 which was filed May 2, 2000, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

Date: November 7, 2000

By: _____

Louis A. Mok
Registration No. 22,585
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　５月　２日

出願番号
Application Number: 特願２０００－１３３４７１

出願人
Applicant (s): 村田機械株式会社
境　隆一
笠原　正雄

２０００年　８月１８日

特許庁長官
Commissioner,
Patent Office 及川耕造

【書類名】　特許願

【整理番号】　21117

【特記事項】　特許法第３０条第１項の規定の適用を受けようとする特許出願

【提出日】　平成12年 5月 2日

【あて先】　特許庁長官殿

【国際特許分類】　G09C 1/00

H04L 9/00

【発明の名称】　鍵共有方法，秘密鍵生成方法，共通鍵生成方法，暗号通信方法，秘密鍵生成器，共通鍵生成器，暗号通信システム及び記録媒体

【請求項の数】　18

【発明者】

【住所又は居所】　京都府京都市山科区大宅辻脇町３７番地の３２

【氏名】　大岸　聖史

【発明者】

【住所又は居所】　京都府京都市山科区安朱東海道町１６－２緑山荘Ｂ棟１０１号室

【氏名】　境　隆一

【発明者】

【住所又は居所】　大阪府箕面市粟生外院４丁目１５番３号

【氏名】　笠原　正雄

【特許出願人】

【識別番号】　000006297

【氏名又は名称】　村田機械株式会社

【代表者】　村田　純一

【特許出願人】

【識別番号】　599100556

【氏名又は名称】　境　隆一

【特許出願人】

【識別番号】　597008636

【氏名又は名称】　笠原　正雄

【代理人】

【識別番号】　100078868

【弁理士】

【氏名又は名称】　河野　登夫

【電話番号】　06-6944-4141

【選任した復代理人】

【識別番号】　100114557

【弁理士】

【氏名又は名称】　河野　英仁

【電話番号】　06-6944-4141

【手数料の表示】

【予納台帳番号】　001889

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9805283

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　鍵共有方法，秘密鍵生成方法，共通鍵生成方法，暗号通信方法，秘密鍵生成器，共通鍵生成器，暗号通信システム及び記録媒体

【特許請求の範囲】

【請求項１】　エンティティ自身の秘密鍵と相手エンティティの公開鍵とを用いて予備通信なしに鍵共有を行う方法において、前記相手エンティティを特定する特定情報に基づき代数曲線上の点に写像したものを前記公開鍵とすることを特徴とする鍵共有方法。

【請求項２】　両エンティティを夫々特定する特定情報に基づき前記両エンティティ間で予備通信なしに鍵共有を行う方法において、代数曲線上で定義されるペアリングを使用することを特徴とする鍵共有方法。

【請求項３】　両エンティティを夫々特定する特定情報に基づき前記両エンティティ間で予備通信なしに鍵共有を行う方法において、一方のエンティティの特定情報に基づき代数曲線上の点に写像したものと秘密情報とから生成された秘密鍵と、他方のエンティティの特定情報に基づき前記代数曲線上の点に写像してなる公開鍵とを用い、前記楕円曲線上で定義されるペアリングを使用して鍵共有を行うことを特徴とする鍵共有方法。

【請求項４】　前記ペアリングは、ベイユペアリングまたはテイトペアリングである請求項２または３記載の鍵共有方法。

【請求項５】　前記代数曲線はその上で定義される離散対数問題を多項式時間で解くことができない請求項１～４の何れかに記載の鍵共有方法。

【請求項６】　一方のエンティティと他方のエンティティとで鍵共有を行う際の夫々のエンティティでの演算処理の過程にあって、互いに逆数の関係になる数値を生成し合う請求項１～５の何れかに記載の鍵共有方法。

【請求項７】　前記各エンティティの特定情報に基づいて複数の公開鍵を生成する請求項１～６の何れかに記載の鍵共有方法。

【請求項８】　エンティティを特定する特定情報に基づいて前記エンティティの秘密鍵を生成する方法において、前記エンティティの特定情報に基づき代数曲線上の点に写像したものと秘密情報とを用いて、前記秘密鍵を生成することを

特徴とする秘密鍵生成方法。

【請求項９】　エンティティを特定する特定情報に基づいて前記エンティティの秘密鍵を生成する方法において、前記エンティティの特定情報に対して一方向性関数を作用させた値に基づき代数曲線上の点に写像したものと秘密情報とを用いて、前記秘密鍵を生成することを特徴とする秘密鍵生成方法。

【請求項１０】　第１エンティティを特定する特定情報に基づく秘密鍵と通信相手の第２エンティティを特定する特定情報に基づく公開鍵とから共通鍵を生成する方法において、前記第１エンティティの特定情報に基づき代数曲線上の点に写像したものと秘密情報とを用いて前記秘密鍵を生成し、前記第２エンティティの特定情報に基づき代数曲線上の点に写像したものを前記公開鍵とすることを特徴とする共通鍵生成方法。

【請求項１１】　前記代数曲線上で定義されるペアリングを使用して前記共通鍵を生成する請求項１０記載の共通鍵生成方法。

【請求項１２】　請求項６記載の鍵共有方法に基づいて共通鍵を生成する方法であって、前記数値における逆数の関係を利用して共通鍵を生成することを特徴とする共通鍵生成方法。

【請求項１３】　センタから各エンティティへ各エンティティの秘密鍵を送付し、一方のエンティティが前記センタから送付された自身の秘密鍵と他方のエンティティの公開鍵とから求めた共通鍵を用いて平文を暗号文に暗号化して前記他方のエンティティへ伝送し、前記他方のエンティティが伝送された暗号文を、前記センタから送付された自身の秘密鍵と前記一方のエンティティの公開鍵とから求めた、前記共通鍵と同一の共通鍵を用いて平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法において、各エンティティを特定する特定情報に基づき代数曲線上の点に写像したものと前記センタ固有の秘密情報とを用いて各エンティティの秘密鍵を生成し、各エンティティの特定情報に基づき代数曲線上の点に写像したものを各エンティティの公開鍵とすることを特徴とする暗号通信方法。

【請求項１４】　エンティティを特定する特定情報に基づいて前記エンティティの秘密鍵を生成する生成器において、前記エンティティの特定情報に基づき

代数曲線上の点に写像して写像値を得る手段と、該写像値と秘密情報とを用いて前記秘密鍵を生成する手段とを備えることを特徴とする秘密鍵生成器。

【請求項１５】　一方のエンティティを特定する特定情報に基づく秘密鍵と通信相手の他方のエンティティを特定する特定情報に基づく公開鍵とから共通鍵を生成する生成器において、前記他方のエンティティの特定情報に基づき代数曲線上の点に写像して前記公開鍵としての写像値を得る手段と、該写像値と前記秘密鍵とを用いて前記共通鍵を生成する手段とを備えることを特徴とする共通鍵生成器。

【請求項１６】　送信すべき情報である平文を暗号文に暗号化する暗号化処理、及び、送信された暗号文を平文に復号する復号処理を、複数のエンティティ間で相互に行うこととし、各エンティティを特定する特定情報に基づいて各エンティティの秘密鍵を生成して各エンティティへ送付するセンタと、該センタから送付された自身の秘密鍵と通信対象のエンティティの特定情報に基づく公開鍵とを用いて前記暗号化処理及び復号処理に使用する共通鍵を生成する複数のエンティティとを有する暗号通信システムにおいて、前記センタにて、各エンティティの特定情報に基づき代数曲線上の点に写像したものと前記センタ固有の秘密情報とを用いて各エンティティの秘密鍵を生成し、各エンティティにて、通信対象のエンティティの特定情報に基づき代数曲線上の点に写像したものを前記公開鍵として前記共通鍵を生成するようにしたことを特徴とする暗号通信システム。

【請求項１７】　コンピュータにエンティティの秘密鍵を生成させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、前記エンティティを特定する特定情報に基づき代数曲線上の点に写像して前記公開鍵としての写像値を得ることをコンピュータに実行させるプログラムコード手段と、前記写像値と秘密情報とを用いて前記秘密鍵を生成することをコンピュータに実行させるプログラムコード手段とを含むプログラムが記録されていることを特徴とする記録媒体。

【請求項１８】　コンピュータに、暗号通信システムにおける平文から暗号文への暗号化処理及び暗号文から平文への復号処理に使用する共通鍵を第１エンティティ側で生成させるためのプログラムが記録されているコンピュータでの読

み取りが可能な記録媒体において、前記第１エンティティの秘密鍵を入力することをコンピュータに実行させるプログラムコード手段と、通信相手の第２エンティティを特定する特定情報に基づき代数曲線上の点に写像して前記公開鍵としての写像値を得ることをコンピュータに実行させるプログラムコード手段と、前記写像値と入力した前記秘密鍵とを用いて前記共通鍵を生成することをコンピュータに実行させるプログラムコード手段とを含むプログラムが記録されていることを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、予備通信なして両エンティティ間で共通鍵を共有し合う鍵共有方法、センタにて各エンティティ固有の秘密鍵を生成する秘密鍵生成方法及び秘密鍵生成器、各エンティティで暗号化処理・復号処理に必要な共通鍵を生成する共通鍵生成方法及び共通鍵生成器、情報の内容が当事者以外にはわからないように暗号文にて通信を行う暗号通信方法及び暗号通信システム、並びに、これらの方法を行うためのプログラムを記録した記録媒体に関する。

【０００２】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事，外交面で用いられてきた暗号技術が注目されている。

【０００３】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換するこ

とである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【０００４】

暗号化鍵と復号鍵とは、等しくても良いし、異なっていても良い。両者の鍵が等しい暗号系は、共通鍵暗号系と呼ばれ、米国商務省標準局が採用したＤＥＳ（Data Encryption Standards)はその典型例である。また、両者の鍵が異なる暗号系の一例として、公開鍵暗号系と呼ばれる暗号系が提案された。この公開鍵暗号系は、暗号系を利用する各ユーザ（エンティティ）が暗号化鍵と復号鍵とを一対ずつ作成し、暗号化鍵を公開鍵リストにて公開し、復号鍵のみを秘密に保持するという暗号系である。公開鍵暗号系では、この一対となる暗号化鍵と復号鍵とが異なり、一方向性関数を利用することによって暗号化鍵から復号鍵を割り出せないという特徴を持たせている。

【０００５】

公開鍵暗号系は、暗号化鍵を公開するという画期的な暗号系であって、高度情報化社会の確立に必要な上述した３つの要素に適合するものであり、情報通信技術の分野等での利用を図るべく、その研究が活発に行われ、典型的な公開鍵暗号系としてＲＳＡ暗号系が提案された。このＲＳＡ暗号系は、一方向性関数として素因数分解の困難さを利用して実現されている。また、離散対数問題を解くことの困難さ（離散対数問題）を利用した公開鍵暗号系も種々の手法が提案されてきた。

【０００６】

また、各エンティティの住所，氏名，電子メールのアドレス等の個人を特定するＩＤ（Identity）情報を利用する暗号系が提案された。この暗号系では、ＩＤ情報に基づいて送受信者間で共通の暗号化・復号鍵を生成する。また、このＩＤ

情報に基づく暗号技法には、（１）暗号文通信に先立って送受信者間での予備通信を必要とする方式と、（２）暗号文通信に先立って送受信者間での予備通信を必要としない方式とがある。特に、（２）の手法は予備通信が不要であるので、エンティティの利便性が高く、将来の暗号系の中枢をなすものと考えられている。

【０００７】

この（２）の手法による暗号系は、ＩＤ－ＮＩＫＳ（ID-based non-interactive key sharing scheme)と呼ばれており、通信相手のＩＤ情報を用いて予備通信を行うことなく暗号化・復号鍵を共有する方式を採用している。ＩＤ－ＮＩＫＳは、送受信者間で公開鍵，秘密鍵を交換する必要がなく、また鍵のリスト及び第三者によるサービスも必要としない方式であり、任意のエンティティ間で安全に通信を行える。

【０００８】

図４は、このＩＤ－ＮＩＫＳのシステムの原理を示す図である。信頼できるセンタの存在を仮定し、このセンタを中心にして共通鍵生成システムを構成している。図４において、エンティティＸの特定情報であるエンティティＸの名前，住所，電話番号，メールアドレス等のＩＤ情報を｛ID_X｝で表す。センタは任意のエンティティＸに対して、センタ公開情報｛PC_i｝，センタ秘密情報｛SC_i｝及びエンティティＸのＩＤ情報｛ID_X｝に基づいて、以下のように秘密情報S_{Xi}を計算し、秘密裏にエンティティＸへ配布する。

$$S_{Xi}=F_i\ (\{SC_i\},\ \{PC_i\},\ \{ID_X\})$$

【０００９】

エンティティＸは他の任意のエンティティＹとの間で、暗号化，復号のための共通鍵K_{XY}を、エンティティＸ自身の秘密情報｛S_{Xi}｝，センタ公開情報｛PC_i｝及び相手先のエンティティＹのＩＤ情報｛ID_Y｝を用いて以下のように生成する。

$$K_{XY}=f\ (\{S_{Xi}\},\ \{PC_i\},\ \{ID_Y\})$$

また、エンティティＹも同様にエンティティＸへの鍵を共通鍵K_{YX}を生成する。もし常に$K_{XY}=K_{YX}$の関係が成立すれば、この鍵K_{XY}，K_{YX}をエンティティＸ，

Ｙ間で暗号化鍵，復号鍵として使用できる。

【００１０】

上述した公開鍵暗号系では、例えばＲＳＡ暗号系の場合にその公開鍵の長さは現在の電話番号の十数倍となり、極めて煩雑である。これに対して、ＩＤ－ＮＩＫＳでは、各ＩＤ情報を名簿という形式で登録しておけば、この名簿を参照して任意のエンティティとの間で共通鍵を生成することができる。従って、図４に示すようなＩＤ－ＮＩＫＳのシステムが安全に実現されれば、多数のエンティティが加入するコンピュータネットワーク上で便利な暗号系を構築できる。このような理由により、ＩＤ－ＮＩＫＳが将来の暗号系の中心になると期待されている。

【００１１】

【発明が解決しようとする課題】

通信相手のＩＤ情報を用いて予備通信を行うことなく暗号化鍵及び復号鍵となる共通鍵を互いに共有するようなＩＤ－ＮＩＫＳにあっては、特に複数のエンティティが結託する結託攻撃に対して十分に安全であることが望まれる。そして、暗号学的に安全なＩＤ－ＮＩＫＳを構築できるか否かは、高度情報化社会にとって重要な問題であり、より理想的な暗号方式の探究が進められている。

【００１２】

本発明は斯かる事情に鑑みてなされたものであり、各エンティティの特定情報（ＩＤ情報）に基づいて、楕円暗号で利用されている楕円曲線等の代数曲線上の点に写像することにより、予備通信を行うことなく両エンティティ間で容易に共通鍵を共有し合える鍵共有方法、この鍵共有方法に基づいて安全なＩＤ－ＮＩＫＳを構築できるための秘密鍵生成方法及び秘密鍵生成器，共通鍵生成方法及び共通鍵生成器，暗号通信方法及び暗号通信システム、並びに、これらの方法を行うためのプログラムを記録した記録媒体を提供することを目的とする。

【００１３】

【課題を解決するための手段】

請求項１に係る鍵共有方法は、エンティティ自身の秘密鍵と相手エンティティの公開鍵とを用いて予備通信なしに鍵共有を行う方法において、前記相手エンティティを特定する特定情報に基づき代数曲線上の点に写像したものを前記公開鍵

とすることを特徴とする。

【００１４】

請求項２に係る鍵共有方法は、両エンティティを夫々特定する特定情報に基づき前記両エンティティ間で予備通信なしに鍵共有を行う方法において、代数曲線上で定義されるペアリングを使用することを特徴とする。

【００１５】

請求項３に係る鍵共有方法は、両エンティティを夫々特定する特定情報に基づき前記両エンティティ間で予備通信なしに鍵共有を行う方法において、一方のエンティティの特定情報に基づき代数曲線上の点に写像したものと秘密情報とから生成された秘密鍵と、他方のエンティティの特定情報に基づき前記代数曲線上の点に写像してなる公開鍵とを用い、前記楕円曲線上で定義されるペアリングを使用して鍵共有を行うことを特徴とする。

【００１６】

請求項４に係る鍵共有方法は、請求項２または３において、前記ペアリングは、ベイユペアリングまたはテイトペアリングであることを特徴とする。

【００１７】

請求項５に係る鍵共有方法は、請求項１～４の何れかにおいて、前記代数曲線はその上で定義される離散対数問題を多項式時間で解くことができないことを特徴とする。

【００１８】

請求項６に係る鍵共有方法は、請求項１～５の何れかにおいて、一方のエンティティと他方のエンティティとで鍵共有を行う際の夫々のエンティティでの演算処理の過程にあって、互いに逆数の関係になる数値を生成し合うことを特徴とする。

【００１９】

請求項７に係る鍵共有方法は、請求項１～６の何れかにおいて、前記各エンティティの特定情報に基づいて複数の公開鍵を生成することを特徴とする。

【００２０】

請求項８に係る秘密鍵生成方法は、エンティティを特定する特定情報に基づい

て前記エンティティの秘密鍵を生成する方法において、前記エンティティの特定情報に基づき代数曲線上の点に写像したものと秘密情報とを用いて、前記秘密鍵を生成することを特徴とする。

【００２１】

請求項９に係る秘密鍵生成方法は、エンティティを特定する特定情報に基づいて前記エンティティの秘密鍵を生成する方法において、前記エンティティの特定情報に対して一方向性関数を作用させた値に基づき代数曲線上の点に写像したものと秘密情報とを用いて、前記秘密鍵を生成することを特徴とする。

【００２２】

請求項１０に係る共通鍵生成方法は、第１エンティティを特定する特定情報に基づく秘密鍵と通信相手の第２エンティティを特定する特定情報に基づく公開鍵とから共通鍵を生成する方法において、前記第１エンティティの特定情報に基づき代数曲線上の点に写像したものと秘密情報とを用いて前記秘密鍵を生成し、前記第２エンティティの特定情報に基づき代数曲線上の点に写像したものを前記公開鍵とすることを特徴とする。

【００２３】

請求項１１に係る共通鍵生成方法は、請求項１０において、前記代数曲線上で定義されるペアリングを使用して前記共通鍵を生成することを特徴とする。

【００２４】

請求項１２に係る共通鍵生成方法は、請求項６記載の鍵共有方法に基づいて共通鍵を生成する方法であって、前記数値における逆数の関係を利用して共通鍵を生成することを特徴とする。

【００２５】

請求項１３に係る暗号通信方法は、センタから各エンティティへ各エンティティの秘密鍵を送付し、一方のエンティティが前記センタから送付された自身の秘密鍵と他方のエンティティの公開鍵とから求めた共通鍵を用いて平文を暗号文に暗号化して前記他方のエンティティへ伝送し、前記他方のエンティティが伝送された暗号文を、前記センタから送付された自身の秘密鍵と前記一方のエンティティの公開鍵とから求めた、前記共通鍵と同一の共通鍵を用いて平文に復号するこ

とにより、エンティティ間で情報の通信を行う暗号通信方法において、各エンティティを特定する特定情報に基づき代数曲線上の点に写像したものと前記センタ固有の秘密情報とを用いて各エンティティの秘密鍵を生成し、各エンティティの特定情報に基づき代数曲線上の点に写像したものを各エンティティの公開鍵とすることを特徴とする。

【００２６】

請求項１４に係る秘密鍵生成器は、エンティティを特定する特定情報に基づいて前記エンティティの秘密鍵を生成する生成器において、前記エンティティの特定情報に基づき代数曲線上の点に写像して写像値を得る手段と、該写像値と秘密情報とを用いて前記秘密鍵を生成する手段とを備えることを特徴とする。

【００２７】

請求項１５に係る共通鍵生成器は、一方のエンティティを特定する特定情報に基づく秘密鍵と通信相手の他方のエンティティを特定する特定情報に基づく公開鍵とから共通鍵を生成する生成器において、前記他方のエンティティの特定情報に基づき代数曲線上の点に写像して前記公開鍵としての写像値を得る手段と、該写像値と前記秘密鍵とを用いて前記共通鍵を生成する手段とを備えることを特徴とする。

【００２８】

請求項１６に係る暗号通信システムは、送信すべき情報である平文を暗号文に暗号化する暗号化処理、及び、送信された暗号文を平文に復号する復号処理を、複数のエンティティ間で相互に行うこととし、各エンティティを特定する特定情報に基づいて各エンティティの秘密鍵を生成して各エンティティへ送付するセンタと、該センタから送付された自身の秘密鍵と通信対象のエンティティの特定情報に基づく公開鍵とを用いて前記暗号化処理及び復号処理に使用する共通鍵を生成する複数のエンティティとを有する暗号通信システムにおいて、前記センタにて、各エンティティの特定情報に基づき代数曲線上の点に写像したものと前記センタ固有の秘密情報とを用いて各エンティティの秘密鍵を生成し、各エンティティにて、通信対象のエンティティの特定情報に基づき代数曲線上の点に写像したものを前記公開鍵として前記共通鍵を生成するようにしたことを特徴とする。

【００２９】

請求項１７に係る記録媒体は、コンピュータにエンティティの秘密鍵を生成させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、前記エンティティを特定する特定情報に基づき代数曲線上の点に写像して前記公開鍵としての写像値を得ることをコンピュータに実行させるプログラムコード手段と、前記写像値と秘密情報とを用いて前記秘密鍵を生成することをコンピュータに実行させるプログラムコード手段とを含むプログラムが記録されていることを特徴とする。

【００３０】

請求項１８に係る記録媒体は、コンピュータに、暗号通信システムにおける平文から暗号文への暗号化処理及び暗号文から平文への復号処理に使用する共通鍵を第１エンティティ側で生成させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、前記第１エンティティの秘密鍵を入力することをコンピュータに実行させるプログラムコード手段と、通信相手の第２エンティティを特定する特定情報に基づき代数曲線上の点に写像して前記公開鍵としての写像値を得ることをコンピュータに実行させるプログラムコード手段と、前記写像値と入力した前記秘密鍵とを用いて前記共通鍵を生成することをコンピュータに実行させるプログラムコード手段とを含むプログラムが記録されていることを特徴とする。

【００３１】

本発明では、各エンティティの特定情報（ＩＤ情報）に基づいて、楕円暗号で利用されている楕円曲線，超楕円曲線等の代数曲線上の点に写像し、その写像値を各エンティティの公開鍵とする。この代数曲線及び写像のアルゴリスムは公開する。センタでは、各エンティティの特定情報（ＩＤ情報）に基づき代数曲線上の点に写像し、その写像値とセンタ自身の秘密情報とを用いて、各エンティティ固有の秘密鍵を生成し、これを対応するエンティティへ秘密裏に送付する。各エンティティは、センタから送られる自身固有の秘密鍵と、通信相手の特定情報（ＩＤ情報）に基づき代数曲線上の点に写像した写像値とを用いて、暗号化処理・復号処理に用いる共通鍵を生成する。この際、楕円曲線上で定義されるペアリン

グ（ベイユ（Weil）ペアリング，テイト（Tate）ペアリング等）を利用して、予備通信を行うことなく、両エンティティ間で同一の共通鍵を共有する。本発明における代数曲線上の点への写像は、各エンティティ，センタの何れでも可能である。

【００３２】

本発明では、安全性の根拠を代数曲線上の離散対数問題（例えば楕円曲線上の離散対数問題、以下、これを単に楕円離散対数問題という）に置いている。複数のエンティティによる結託攻撃にて本発明の暗号システムが破られることは、例えば楕円離散対数問題が解かれることと等価であるかまたはそれ以上に困難であり、その安全性は極めて高い。

【００３３】

【発明の実施の形態】

本発明の実施の形態について具体的に説明する。

図１は、本発明の暗号通信システムの構成を示す模式図である。情報の隠匿を信頼できるセンタ１が設定されており、このセンタ１としては、例えば社会の公的機関を該当できる。このセンタ１と、この暗号通信システムを利用するユーザとしての複数の各エンティティＡ，Ｂ，…，Ｚとは、秘密通信路２ａ，２ｂ，…，２ｚにより接続されており、これらの秘密通信路２ａ，２ｂ，…，２ｚを介してセンタ１から秘密の鍵情報（秘密鍵S_a，S_b，…，S_z）が各エンティティＡ，Ｂ，…，Ｚへ伝送されるようになっている。また、２人のエンティティの間には通信路３ab，３az，３bz，…が設けられており、この通信路３ab，３az，３bz，…を介して通信情報を暗号化した暗号文が互いのエンティティ間で伝送されるようになっている。

【００３４】

以下、代数曲線として楕円曲線を用いる場合の本発明における基本方式について説明する。

まず、本発明で用いる楕円曲線のベイユペアリングの基本的性質を述べる。ベイユペアリングは、楕円曲線上の点がなす群Ｅ／F_qから有限体上F_d（但し，$d=q^k$）の乗法群への写像である。ベイユペアリングには、以下に示すよう双

線形性と交換則とが成り立つ。なお、（．）はペイユペアリングを表し、Ｐ，Ｐ$_1$，Ｐ$_2$，Ｑ，Ｑ$_1$，Ｑ$_2$は楕円曲線上の点を示す。

【００３５】

（双線形性）

$$(P_1 + P_2 . Q) = (P_1 . Q)(P_2 . Q)$$

$$(P . Q_1 + Q_2) = (P . Q_1)(P . Q_2)$$

（交換則）

$$(P . Q) = (Q . P)^{-1}$$

双線形性を有するので、ｍを整数とした場合、以下のような等式が成立する。

$$(mP . Q) = (P . Q)^m$$

$$(P . mQ) = (P . Q)^m$$

【００３６】

ペイユペアリングに基づく鍵共有法を以下に説明する。

（センタ１での秘密鍵生成）

任意のエンティティＡの名前，住所，電話番号，メールアドレス等の特定情報（ＩＤ情報）をＩＤ$_a$とする。センタ１は、ペイユペアリングのアルゴリズム（．）と任意のエンティティＡのＩＤ情報ＩＤ$_a$を楕円曲線上の点Ｐ$_a$∈Ｅ／Ｆ$_q$に変換して（写像して）公開鍵を求める関数ｆ（）とを公開する。また、センタ１は、秘密の乱数ｒを生成し、この乱数ｒとエンティティＡの公開鍵Ｐ$_a$とを用いて下記（１）のようにエンティティＡの秘密鍵Ｓ$_a$を求め、求めた秘密鍵Ｓ$_a$を秘密裏にエンティティＡへ配布する。

$$S_a = r P_a \qquad \cdots (1)$$

【００３７】

以上のような秘密情報，公開情報をまとめると、次のようになる。

センタ１の公開情報　　：（．），ｆ（）

センタ１の秘密情報　　：ｒ（ランダムな整数）

エンティティＡの公開鍵：Ｐ$_a$（＝ｆ（ＩＤ$_a$））

エンティティＡの秘密鍵：Ｓ$_a$（＝ｒ・ｆ（ＩＤ$_a$））

【００３８】

（エンティティＡ，Ｂでの共通鍵生成）

各エンティティは、センタ１から配布された自身の秘密鍵と通信相手であるエンティティの公開鍵とから、楕円曲線上でのペイユペアリングを利用して、共通鍵を生成する。

（第１例）

エンティティＡのＩＤ情報$ＩＤ_a$とエンティティＢのＩＤ情報$ＩＤ_b$との間での大小比較を行えるアルゴリスムを設定し、ペアリングを計算する際にその大小情報を用いてペアリングの順序を適切に設定する。このアルゴリスムとしては、辞書式または２進数で表したときの大小などが可能である。なお、ペアリングの順序を設定する方法として、ＩＤ情報$ＩＤ_a$，$ＩＤ_b$を変換（写像）した後の公開鍵$Ｐ_a$，$Ｐ_b$の大小情報を用いることも可能である。

【００３９】

例えば、$ＩＤ_a > ＩＤ_b$である場合、エンティティＡは、自身の秘密鍵$Ｓ_a$と、エンティティＢのＩＤ情報$ＩＤ_b$を楕円曲線に写像した公開鍵$Ｐ_b$とを用いて、下記（２）に従って共通鍵$Ｋ_{ab}$を生成する。

$$Ｋ_{ab}＝（Ｓ_a \cdot Ｐ_b）$$
$$＝（ｒＰ_a \cdot Ｐ_b）$$
$$＝（Ｐ_a \cdot Ｐ_b）^{r} \quad \cdots（２）$$

【００４０】

一方、$ＩＤ_a > ＩＤ_b$である場合、エンティティＢは、エンティティＡのＩＤ情報$ＩＤ_a$を楕円曲線に写像した公開鍵$Ｐ_a$と自身の秘密鍵$Ｓ_b$とを用いて、下記（３）に従って共通鍵$Ｋ_{ba}$を生成する。

$$Ｋ_{ba}＝（Ｐ_a \cdot Ｓ_b）$$
$$＝（Ｐ_a \cdot ｒＰ_b）$$
$$＝（Ｐ_a \cdot Ｐ_b）^{r} \quad \cdots（３）$$

よって、エンティティＡが生成する共通鍵$Ｋ_{ab}$とエンティティＢが生成する共通鍵$Ｋ_{ba}$とは一致して、両エンティティＡ，Ｂ間で共通鍵を共有できる。

【００４１】

以下に、上記のようなＩＤ情報の大小関係を設定しないで鍵共有を可能とする

２つの例について説明する。

【００４２】

（第２例）

ｘ，ｙに関する対称関数ｇ（ｘ，ｙ）（但し、ｇ（ｘ，ｙ）＝ｘｙは除く）を設定する。以下の例では、ｇ（ｘ，ｙ）＝ｘ＋ｙとする。エンティティＡは、ｇ（ｘ，ｙ）＝ｘ＋ｙに従って下記（４）のように、共通鍵$K_{ab}=k_{ab}+k_{ba}$を生成する。

$$\begin{aligned}K_{ab}&=k_{ab}+k_{ba}\\&=(S_a\cdot P_b)+(P_b\cdot S_a)\\&=(rP_a\cdot P_b)+(P_b\cdot rP_a)\\&=(P_a\cdot P_b)^r+(P_b\cdot P_a)^r \qquad \cdots(4)\end{aligned}$$

【００４３】

一方、エンティティＢは、ｇ（ｘ，ｙ）＝ｘ＋ｙに従って下記（５）のように、共通鍵$K_{ba}=k_{ba}+k_{ab}$を生成する。

$$\begin{aligned}K_{ba}&=k_{ba}+k_{ab}\\&=(S_b\cdot P_a)+(P_a\cdot S_b)\\&=(rP_b\cdot P_a)+(P_a\cdot rP_b)\\&=(P_b\cdot P_a)^r+(P_a\cdot P_b)^r \qquad \cdots(5)\end{aligned}$$

よって、エンティティＡが生成する共通鍵K_{ab}とエンティティＢが生成する共通鍵K_{ba}とは一致して、両エンティティＡ，Ｂ間で共通鍵を共有できる。なお、他の種類の対称関数ｇ（ｘ，ｙ）を利用しても、同様に鍵共有が可能である。

【００４４】

（第３例）

エンティティＡは、第２例で示したk_{ab}を用いて、下記（６）のように、共通鍵$K_{ba}=k_{ab}+k_{ab}^{-1}$を生成する。

$$\begin{aligned}K_{ba}&=k_{ab}+k_{ab}^{-1}\\&=(S_a\cdot P_b)+(S_a\cdot P_b)^{-1}\\&=(rP_a\cdot P_b)+(rP_a\cdot P_b)^{-1}\\&=(P_a\cdot P_b)^r+(P_a\cdot P_b)^{-r} \qquad \cdots(6)\end{aligned}$$

【００４５】

エンティティＢは、第２例で示したk_{ba}を用いて、下記（７）のように、共通鍵$K_{ba}=k_{ba}+k_{ba}^{-1}$を生成する。

$$K_{ba}=k_{ba}+k_{ba}^{-1}$$
$$=(S_b \cdot P_a)+(S_b \cdot P_a)^{-1}$$
$$=(rP_b \cdot P_a)+(rP_b \cdot P_a)^{-1}$$
$$=(P_b \cdot P_a)^{r}+(P_b \cdot P_a)^{-r}$$
$$=(P_a \cdot P_b)^{-r}+(P_a \cdot P_b)^{r} \quad \cdots (7)$$

よって、エンティティＡが生成する共通鍵K_{ab}とエンティティＢが生成する共通鍵K_{ba}とは一致して、両エンティティＡ，Ｂ間で共通鍵を共有できる。

【００４６】

以上のようにして、ベイユペアリングを利用して、各エンティティ間で等しい共通鍵を容易に生成できる。

【００４７】

なお、上述した例では、エンティティＡのＩＤ情報ID_aから直接に写像点P_aを求めるようにしたが、一方向性関数を用いてＩＤ情報ID_aを変換し、その変換値から写像点P_aを求めるようにしても良い。この際、一方向性関数の例としてハッシュ関数ｈ（）を用いた場合、公開鍵$P_a=f(h(ID_a))$，秘密鍵$S_a=r \cdot f(h(ID_a))$となる。

【００４８】

エンティティが、センタ１の秘密情報ｒを求めることを困難にするためには、次の２つの条件が必要である。

（条件１）ｑを2^{160}以上に設定すること。

（条件２）$\#E/F_q \mid q^k-1$かつ$q^k>2^{1024}$を満たすような整数ｋが存在すること。

【００４９】

（条件１）は、楕円離散対数問題を求めることを困難にするために必要である。（条件２）は、有限体F_d（但し，$d=q^k$）の離散対数問題を求めることを困難にするために必要である。

【００５０】

次に、上述した鍵共有方式を利用した暗号システムにおけるエンティティ間の情報通信について説明する。図２は、２人のエンティティＡ，Ｂ間における情報の通信状態を示す模式図である。図２の例は、エンティティＡが平文（メッセージ）Ｍを暗号文Ｃに暗号化してそれをエンティティＢへ伝送し、エンティティＢがその暗号文Ｃを元の平文（メッセージ）Ｍに復号する場合を示している。

【００５１】

センタ１には、関数ｆ（）を用いて、各エンティティＡ，ＢのＩＤ情報$ＩＤ_a$，$ＩＤ_b$を楕円曲線に写像した写像位置である公開鍵$Ｐ_a$，$Ｐ_b$を得る公開鍵生成器１ａと、その公開鍵$Ｐ_a$，$Ｐ_b$とセンタ固有の秘密情報ｒとを用いて各エンティティＡ，Ｂの秘密鍵$Ｓ_a$，$Ｓ_b$を求める秘密鍵生成器１ｂとが備えられている。そして、センタ１から各エンティティＡ，Ｂへ、前記（１）に従って生成された秘密鍵$Ｓ_a$，$Ｓ_b$が送付される。

【００５２】

エンティティＡ側には、エンティティＢのＩＤ情報$ＩＤ_b$を入力し、それを楕円曲線に写像した写像位置である公開鍵$Ｐ_b$を得る公開鍵生成器１１と、センタ１から送られる秘密鍵$Ｓ_a$と公開鍵生成器１１からの公開鍵$Ｐ_b$とに基づいてエンティティＡが求めるエンティティＢとの共通鍵$Ｋ_{ab}$を生成する共通鍵生成器１２と、共通鍵$Ｋ_{ab}$を使用して平文（メッセージ）Ｍを暗号文Ｃに暗号化して通信路３０へ出力する暗号化器１３とが備えられている。

【００５３】

また、エンティティＢ側には、エンティティＡのＩＤ情報$ＩＤ_a$を入力し、それを楕円曲線に写像した写像位置である公開鍵$Ｐ_a$を得る公開鍵生成器２１と、センタ１から送られる秘密鍵$Ｓ_b$と公開鍵生成器２１からの公開$Ｐ_a$とに基づいてエンティティＢが求めるエンティティＡとの共通鍵$Ｋ_{ba}$を生成する共通鍵生成器２２と、通信路３０から入力した暗号文Ｃを共通鍵$Ｋ_{ba}$を使用して平文（メッセージ）Ｍに復号して出力する復号器２３とが備えられている。

【００５４】

次に、動作について説明する。エンティティＡからエンティティＢへ情報を伝

送しようとする場合、まず、エンティティＢのＩＤ情報$ＩＤ_b$が公開鍵生成器１１に入力されて公開鍵$Ｐ_b$が得られ、得られた公開鍵$Ｐ_b$が共通鍵生成器１２へ送られる。また、センタ１から秘密鍵$Ｓ_a$が共通鍵生成器１２へ入力される。そして、前記（２），（４）または（６）に従って共通鍵$Ｋ_{ab}$が求められて、暗号化器１３へ送られる。暗号化器１３において、この共通鍵$Ｋ_{ab}$を用いて平文（メッセージ）Ｍが暗号文Ｃに暗号化され、暗号文Ｃが通信路３０を介して伝送される。

【００５５】

通信路３０を伝送された暗号文Ｃはエンティティの復号器２３へ入力される。エンティティＡのＩＤ情報$ＩＤ_a$が公開鍵生成器２１に入力されて公開鍵$Ｐ_a$が得られ、得られた公開鍵$Ｐ_a$が共通鍵生成器２２へ送られる。また、センタ１から秘密鍵$Ｓ_b$が共通鍵生成器２２へ入力される。そして、前記（３），（５）または（７）に従って共通鍵$Ｋ_{ba}$が求められて、復号器２３へ送られる。復号器２３において、この共通鍵$Ｋ_{ba}$を用いて暗号文Ｃが平文（メッセージ）Ｍに復号される。

【００５６】

次に、本発明における安全性について説明する。本発明の安全性は、楕円離散対数問題と後述するようにこれと等価である拡張楕円離散対数問題とに基づいている。

【００５７】

〔楕円離散対数問題と拡張楕円離散対数問題との等価性〕

通常の楕円離散対数問題とは、楕円曲線Ｅ上の任意の点Ｐとその$ｒ$倍点$Ｑ＝ｒＰ$が与えられている場合に、Ｐ，Ｑから$ｒ$を求める問題である。ここで、下記（８）のように、楕円曲線上の任意の点$Ｐ_i$（$１\leqq ｉ\leqq ｎ－１$）とその点$Ｐ_i$に基づくＱが与えられている場合に、ある１組の$ｒ_i$（$１\leqq ｉ\leqq ｎ－１$）を求める問題を拡張楕円離散対数問題と定義する。楕円離散対数問題と拡張楕円離散対数問題との等価性について考察する。なお．議論の簡単化のために楕円曲線は素数位数$ｐ$とする。

【００５８】

【数１】

$$P_i, Q(=\sum_{i=1}^{n-1} r_i P_i) \rightarrow r_i \ (1 \leqq \forall_i \leqq n-1) \cdots (8)$$

【００５９】

（楕円離散対数問題から拡張楕円離散対数問題への帰着）

楕円離散対数問題がベースポイントＰを基準として解けると仮定する。P_i（１≦ｉ≦ｎ－１）及びＱは、夫々楕円曲線上のベースポイントＰを基準として係数を、下記（９）のように求めることができる。

【００６０】

【数２】

$$P_i \rightarrow r'_i \quad \text{但し } P_i = r'_i P \ (1 \leqq \forall_i \leqq n-1)$$

$$\sum_{i=1}^{n-1} r_i P_i \rightarrow r' \quad \text{但し } \sum_{i=1}^{n-1} r_i P_i = r'P \qquad \cdots (9)$$

【００６１】

係数r_i'，r'をF_pの元として、下記（10）の不定方程式を解くことにより、r_i（１≦ｉ≦ｎ－１）を求めることが可能である。よって、拡張楕円離散対数問題を解くことができる。

【００６２】

【数３】

$$r' = \sum_{i=1}^{n-1} r_i r'_i \qquad \cdots (10)$$

【００６３】

（拡張楕円離散対数問題から楕円離散対数問題への帰着）

任意の拡張楕円離散対数問題が解けると仮定する。ここで、楕円曲線上の点P_i（１≦ｉ≦ｎ）に対して、下記（11）で示される拡張楕円離散対数問題を解き

、これを行列を用いて表すと下記（12）のようになる。

【００６４】

【数４】

$$P_i = \sum_{\substack{j=1 \\ j \neq i}}^{n} r_{i,j} P_j \quad (1 \leqq i \leqq n) \cdots (11)$$

$$\begin{pmatrix} r_{1,1}P_1 & r_{1,2}P_2 & \cdots & r_{1,n-1}P_{n-1} & -P_n \\ r_{2,1}P_1 & r_{2,2}P_2 & \cdots & -P_{n-1} & r_{2,n}P_n \\ \vdots & \vdots & & \vdots & \vdots \\ -P_1 & r_{n,2}P_2 & \cdots & r_{n,n-1}P_{n-1} & r_{n,n}P_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \cdots (12)$$

【００６５】

上記（12）の行列について係数のみを抜き出すと下記（13）のような関係式が得られ、下記（14）のように変形可能である。

【００６６】

【数５】

$$\begin{pmatrix} r_{1,1} & r_{1,2} & \cdots & r_{1,n-1} & -1 \\ r_{2,1} & r_{2,2} & \cdots & -1 & r_{2,n} \\ \vdots & \vdots & & \vdots & \vdots \\ -1 & r_{n,2} & \cdots & r_{n,n-1} & r_{n,n} \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \pmod{p} \quad \cdots (13)$$

$$\begin{pmatrix} -1 & 0 & \cdots & 0 & r'_1 \\ 0 & -1 & \cdots & 0 & r'_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & r'_{n-1} \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} \pmod{p} \quad \cdots (14)$$

【００６７】

上記（14）から分かるように、点P_i（$1 \leqq i \leqq n-1$）はをP_nの定数倍で表すことが可能である。即ち、拡張楕円離散対数問題を解くことによって、$P_i = r_i' P_n$を満たすr_i'を求めることができる。

以上のことから、楕円離散対数問題と拡張楕円離散対数問題とは等価になる。

【００６８】

〔センタの秘密情報に関する安全性〕

エンティティＣの公開鍵P_cと秘密鍵S_cとからセンタの秘密情報ｒを得ることは、楕円離散対数問題を解くことと等価であって、困難である。

エンティティＡの公開鍵P_aとエンティティＢの公開鍵P_bとから（$P_a \cdot P_b$）を計算し、これと共通鍵$K_{ab} = (P_a \cdot P_b)^r$とからｒを得ることは離散対数問題を解くことと等価であって、困難である。

よって、どのエンティティもセンタの秘密情報ｒを求めることができない。

【００６９】

〔エンティティの秘密鍵に関する安全性〕

ｎ人のエンティティが結託してエンティティＣの秘密鍵S_cを偽造する攻撃に

ついて考察する。エンティティＣの公開鍵P_cが下記（15）のように他のエンティティの公開鍵の線形結合によって表すことが可能であると仮定すると、前記（1）にこの線形結合を代入すると、下記（16）の関係式が成立するので、エンティティＣの秘密鍵S_cが露呈する。

$$P_c = u_1 P_1 + u_2 P_2 + \cdots + u_n P_n \quad \cdots (15)$$

$$\begin{aligned} S_c &= r P_c \\ &= r (u_1 P_1 + u_2 P_2 + \cdots + u_n P_n) \\ &= u_1 (r P_1) + u_2 (r P_2) + \cdots + u_n (r P_n) \\ &= u_1 S_1 + u_2 S_2 + \cdots + u_n S_n \quad \cdots (16) \end{aligned}$$

【００７０】

しかし、上記（15）での係数u_iを得るには拡張楕円離散対数問題を解く必要があり、このような攻撃は困難であるといえる。よって、安全性は拡張楕円離散対数問題を解くことの難しさに基づいている。

【００７１】

ここで、この秘密鍵の安全性について更に詳述する。拡張楕円離散対数問題は、ＰをE/F_q上の任意の点、（G_1，G_2）をE/F_qの生成元とした場合に、下記（17）において係数u_1，u_2を求める問題である。

$$P = u_1 G_1 + u_2 G_2 \quad \cdots (17)$$

【００７２】

G_1，G_2の次数を＃（G_1），＃（G_2）と定義する。但し、＃（G_1）｜＃（G_2）とする。拡張楕円離散対数問題が解けるとすれば、$P = u_1 G_1 + u_2 G_2$での係数u_1，u_2及び$Q = v_1 G_1 + v_2 G_2$での係数v_1，v_2は求まり、楕円離散対数問題Ｑ＝ｒＰは、下記（18）のように解ける。

【００７３】

【数６】

$$rU_1 \equiv V_1 \ (\mathrm{mod}\#(G_1))$$

$$rU_2 \equiv V_2 \ (\mathrm{mod}\#(G_2))$$

$$r \equiv \frac{V_1}{U_1}\left(\mathrm{mod}\ \frac{\#(G_1)}{gcd(u_1, \#(G_1))}\right)$$

$$r \equiv \frac{V_2}{U_2}\left(\mathrm{mod}\ \frac{\#(G_2)}{gcd(u_2, \#(G_2))}\right) \quad \cdots (18)$$

【００７４】

上記（15）を解く問題と拡張楕円離散対数問題との等価性について考察する。上記（15）が解けたとすると、下記（19）の$r_{i,j}$を求めることができる。

【００７５】

【数７】

$$P_i = \sum_{\substack{j=1 \\ j \neq i}}^{n} r_{i,j} P_j \ (1 \leqq i \leqq n-2) \cdots (19)$$

【００７６】

そして、下記（20）の式において、左辺の（ｎ－２）×（ｎ－２）の行列式が、$P_{n-1} = G_1$，$P_n = G_2$である＃（G_2）に素であるという仮定のもとで、その下記（20）の式を解くことができる。行列式が＃（G_2）に素でない場合には、上記（19）の別の解$r_{i,j}$を選択できる。

【００７７】

【数８】

$$\begin{pmatrix} -1 & r_{1,2} & \cdots & r_{1,n-2} \\ r_{2,1} & -1 & \cdots & -r_{2,n-2} \\ \vdots & \vdots & & \vdots \\ r_{n-2,1} & r_{n-2,2} & \cdots & -1 \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \\ \vdots \\ P_{n-2} \end{pmatrix}$$

$$= -\begin{pmatrix} r_{1,n-1} & r_{1,n} \\ r_{2,n-1} & r_{2,n} \\ \vdots & \vdots \\ r_{n-2,n-1} & r_{n-2,n} \end{pmatrix} \begin{pmatrix} P_{n-1} \\ P_n \end{pmatrix} \cdots (20)$$

【００７８】

この結果、上記（15）が解けるとすれば、下記（21）に示すP_iと（G_1，G_2）との拡張楕円離散対数問題も解ける。

【００７９】

【数９】

$$\begin{pmatrix} P_1 \\ P_2 \\ \vdots \\ P_{n-2} \end{pmatrix} = \begin{pmatrix} r'_{1,n-1} & r'_{1,n} \\ r'_{2,n-1} & r'_{2,n} \\ \vdots & \vdots \\ r'_{n-2,n-1} & r'_{n-2,n} \end{pmatrix} \begin{pmatrix} P_{n-1} \\ P_n \end{pmatrix} \cdots (21)$$

【００８０】

これとは逆に、拡張楕円離散対数問題が解ければ、上記（15）が解けることを示す。P_iと（G_1，G_2）との拡張楕円離散対数問題を下記（22）のように定義し、P_Cと（G_1，G_2）との拡張楕円離散対数問題を下記（23）のように定義すると、下記（24）に示すような関係が成立する。

【００８１】

【数１０】

$$\begin{pmatrix} P_1 \\ P_2 \\ \vdots \\ P_n \end{pmatrix} = \begin{pmatrix} r_{1,1} & r_{1,2} \\ r_{2,1} & r_{2,2} \\ \vdots & \vdots \\ r_{n,1} & r_{n,2} \end{pmatrix} \begin{pmatrix} G_1 \\ G_2 \end{pmatrix} \cdots (22)$$

$$Pc = v_1 G_1 + v_2 G_2 \quad \cdots (23)$$

$$\left.\begin{aligned} v_1 G_1 + v_2 G_2 &= \sum_{i=1}^{n} u_i r_{i,1} G_1 + \sum_{i=1}^{n} u_i r_{i,2} G_2 \\ v_1 &= \sum_{i=1}^{n} u_i r_{i,1} \\ v_2 &= \sum_{i=1}^{n} u_i r_{i,2} \end{aligned}\right\} \cdots (24)$$

【００８２】

v_j と $r_{i,j}$ が与えられている場合には、u_i が解けることは明らかである。よって、上記（15）を解く問題と拡張楕円離散対数問題とは等価である。また、楕円曲線の群が周期的である場合、拡張楕円離散対数問題が楕円離散対数問題と等価であることは明らかである。よって、この場合、上記（15）を解く問題は楕円離散対数問題と等価になる。

【００８３】

〔エンティティ間の共通鍵に関する安全性〕

ｎ人のエンティティの結託により、エンティティＡ，エンティティＣ間の共通鍵を偽造する攻撃について考察する。エンティティＣの公開鍵 P_c が上記（15）のように他のエンティティの公開鍵の線形結合によって表すことが可能であると仮定すると、下記（25），（26）のように、両エンティティＡ，Ｃ間の共通鍵 K_{ac}，K_{ca} が露呈する。エンティティＣの秘密鍵 S_c が線形結合により書き表せる場合も同様に考えられる。

【００８４】

【数１１】

$$K_{ac} = (S_a . P_c)$$
$$= (S_a . u_1 P_1 + u_2 P_2 + \cdots + u_n P_n)$$
$$= (S_a . P_1)^{u_1} (S_a . P_2)^{u_2} \cdots (S_a . P_n)^{u_n}$$
$$= K_{a1}^{u_1} K_{a2}^{u_2} \cdots K_{an}^{u_n} \cdots (25)$$

$$K_{ca} = K_{1a}^{-u_1} K_{2a}^{-u_2} \cdots K_{na}^{-u_n} \cdots (26)$$

【００８５】

しかしながら、上記（15）での係数u_iを求めるには拡張楕円離散対数問題を解くことになり、このような攻撃は困難である。

【００８６】

もし、エンティティＡが自身の公開鍵P_a，秘密鍵S_aから他のエンティティ間の共通鍵K_{bc}を偽造しようとしても不可能である。なぜなら、秘密鍵S_b，S_cはエンティティＢ，Ｃの秘密情報であり、それらは秘密情報ｒなしでは求められないからである。よって、どのエンティティも共通鍵K_{bc}を偽造できない。

【００８７】

秘密鍵S_b，S_cなしに結託エンティティＩの秘密鍵S_iから共通鍵K_{bc}を求める結託攻撃は、秘密鍵S_iから秘密鍵S_b，S_cを求める場合と同じ問題になる。また、結託エンティティＩ，Ｊ間の共通鍵K_{ij}から共通鍵K_{bc}を求める結託攻撃は、センタの秘密情報ｒを知らないので、困難な問題となる。共通鍵K_{bc}を求める問題は、Diffe-Hellman 型問題に帰着する。

【００８８】

ところで、エンティティＡは共通鍵K_{ab}，K_{ac}を算出することが可能であるので、共通鍵K_{ab}，K_{ac}から共通鍵K_{bc}を求めることができるとすれば、エンティティＡは他エンティティ間の共通鍵を偽造可能である。しかし、このような攻撃法は本発明には適用困難である。

【００８９】

以下、本発明の他の実施の形態である、各エンティティのＩＤ情報をベクトルに拡張した鍵共有方式について説明する。

【００９０】

エンティティＡのＩＤ情報であるベクトルP_aを下記（27）のように表す。

ベクトル$P_a = (P_{a1}, P_{a2}, \cdots, P_{an})$　　…（27）

また、センタ１の秘密情報としてｎ×ｎの対称行列Ｒを下記（28）のように設定する。

【００９１】

【数１２】

$$R = R^t = \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nn} \end{pmatrix} \cdots (28)$$

【００９２】

センタ１は、このベクトルP_a及び対称行列Ｒを用い、下記（29）に従って、エンティティＡの秘密鍵（ベクトルS_a）を求め、求めた秘密鍵を秘密裏にエンティティＡへ送付する。

【００９３】

【数１３】

$$\overrightarrow{S_a} = \overrightarrow{P_a} R \cdots (29)$$

【００９４】

エンティティＡは、エンティティＢとの共通鍵を、下記（30）に従って、共通鍵K_{ab}を生成する。但し、点と点との積はペイユペアリングの値とする。

【００９５】

【数１４】

$$
\begin{aligned}
&K_{ab} \\
&= \overrightarrow{S_a}\,\overrightarrow{P_b}^{\,t} \\
&= \overrightarrow{P_a}\,R\,\overrightarrow{P_b}^{\,t} \\
&= \begin{pmatrix} P_{a1} P_{a2} \cdots P_{an} \end{pmatrix} \begin{pmatrix} r_{11} & r_{12} \cdots r_{1n} \\ r_{21} & r_{22} \cdots r_{2n} \\ \vdots & \vdots \quad \vdots \\ r_{n1} & r_{n2} \cdots r_{nn} \end{pmatrix} \begin{pmatrix} P_{b1} \\ P_{b2} \\ \vdots \\ P_{bn} \end{pmatrix} \\
&= \left(\sum_{i=1}^{n} r_{i1} P_{ai} \sum_{i=1}^{n} r_{i2} P_{ai} \cdots \sum_{i=1}^{n} r_{in} P_{ai} \right) \begin{pmatrix} P_{b1} \\ P_{b2} \\ \vdots \\ P_{bn} \end{pmatrix} \\
&= \prod_{j=1}^{n} \left(\sum_{i=1}^{n} r_{ij} P_{ai} . P_{bj} \right) \\
&= \prod_{j=1}^{n} \prod_{i=1}^{n} \left(P_{ai} . P_{bj} \right)^{r_{ij}} \qquad \cdots (30)
\end{aligned}
$$

【００９６】

また、エンティティＢは、エンティティＡとの共通鍵K_{ba}を同様に生成する。そして、前述した実施の形態の第１例のように各エンティティＡ，Ｂ間のＩＤ情報の大小関係を考慮するようにした場合には、$K_{ab}=K_{ba}$となり、同一の共通鍵を共有し合うことができる。

【００９７】

次に、この実施の形態における安全性について考察する。

〔センタの秘密情報に関する安全性〕

エンティティＣの公開鍵ベクトルP_cと秘密鍵ベクトルS_cとからセンタの秘密行列Ｒを得ることは、拡張楕円離散対数問題を解くことと等価であって、困難である。

エンティティＡの公開鍵ベクトルP_aとエンティティＢの公開鍵ベクトルP_b

とから（P_{ai}. P_{bj}）（１≦ｉ，ｊ≦ｎ）を計算し、これと下記（31）に示す共通鍵K_{ab}とから行列Ｒの各成分r_{ij}（１≦ｉ，ｊ≦ｎ）を得ることは、拡張楕円離散対数問題が楕円離散対数問題とが等価であることと同様に、拡張離散対数問題と離散対数問題とで等価である。

【００９８】

【数１５】

$$K_{ab} = \prod_{j=1}^{n} \prod_{i=1}^{n} \left(P_{ai} . P_{bj} \right)^{r_{ij}} \quad \cdots (31)$$

【００９９】

以上のことから、センタ１の秘密情報（対称行列Ｒ）は露呈しない。

【０１００】

〔エンティティの秘密鍵に関する安全性〕

ｎ人のエンティティが結託してエンティティＣの秘密鍵ベクトルS_cを偽造する攻撃について考察する。エンティティＣの公開鍵ベクトルP_cが下記（32）のように他のエンティティの公開鍵ベクトルの線形結合によって表すことが可能であると仮定すると、前記（29）にこの線形結合を代入すると、下記（33）の関係式が成立するので、エンティティＣの秘密鍵ベクトルS_cが露呈する。

【０１０１】

【数１６】

$$\overrightarrow{P_C} = u_1\overrightarrow{P_1}+u_2\overrightarrow{P_2}+\cdots+u_n\overrightarrow{P_n} \quad \cdots(32)$$

$$\begin{aligned}\overrightarrow{S_C} &= \overrightarrow{P_C}R \\ &= \left(u_1\overrightarrow{P_1}+u_2\overrightarrow{P_2}+\cdots+u_n\overrightarrow{P_n}\right)R \\ &= u_1\left(\overrightarrow{P_1}R\right)+u_2\left(\overrightarrow{P_2}R\right)+\cdots+u_n\left(\overrightarrow{P_n}R\right) \\ &= u_1\overrightarrow{S_1}+u_2\overrightarrow{S_2}+\cdots+u_n\overrightarrow{S_n} \quad \cdots(33)\end{aligned}$$

【０１０２】

しかし、前記（29）での成分を得るには拡張楕円離散対数問題を解く必要があり、このような攻撃は困難であるといえる。よって、安全性は拡張楕円離散対数問題を解くことの難しさに基づいている。

【０１０３】

〔エンティティ間の共通鍵に関する安全性〕

ｎ人のエンティティの結託により、エンティティＡ，エンティティＣ間の共通鍵を偽造する攻撃について考察する。エンティティＣの公開鍵ベクトルP_cが上記（32）のように他のエンティティの公開鍵ベクトルの線形結合によって表すことが可能であると仮定すると、下記（34），（35）のように、両エンティティＡ，Ｃ間の共通鍵K_{ac}，K_{ca}が露呈する。エンティティＣの秘密鍵ベクトルS_cが線形結合により書き表せる場合も同様に考えられる。

【０１０４】

【数１７】

$$K_{ac} = \overrightarrow{S_a}\,\overrightarrow{P_c}$$
$$= \overrightarrow{S_a}\left(u_1\overrightarrow{P_1}+u_2\overrightarrow{P_2}+\cdots+u_n\overrightarrow{P_n}\right)$$
$$= (\overrightarrow{S_aP_1})^{u_1}(\overrightarrow{S_aP_2})^{u_2}\cdots(\overrightarrow{S_aP_n})^{u_n}$$
$$= K_{a1}^{u_1}K_{a2}^{u_2}\cdots K_{an}^{u_n} \qquad \cdots (34)$$

$$K_{ca} = K_{1a}^{-u_1}K_{2a}^{-u_2}\cdots K_{na}^{-u_n} \qquad \cdots (35)$$

【０１０５】

しかしながら、上記（32）での係数u_iを求めるには拡張楕円離散対数問題を解くことになり、このような攻撃は困難である。

【０１０６】

また、この実施の形態にあっても、上述した実施の形態と同様に、あるエンティティが自身の共通鍵から他のエンティティ同士間の共通鍵を生成することは困難である。

【０１０７】

なお、エンティティのＩＤ情報をｎ×ｎの対称行列に拡張することも可能である。この場合、共通鍵行列$k_{ab}=(s_{ij})$と共通鍵行列$k_{ba}=(t_{ji})$とは、下記（36）の関係を満たす。

$$s_{ij}=t_{ji}^{-1} \qquad \cdots (36)$$

【０１０８】

なお、上述した例ではベイユペアリングを用いる場合について説明したが、楕円曲線上のペアリングとしてテイト（Ｔａｔｅ）ペアリングを利用する場合にあっても、同様に両エンティティ間で鍵共有を行える。

【０１０９】

また、ベイユペアリング及びテイトペアリングの何れの場合にあっても、鍵共有を行う際のペアリング（Ｐ．Ｑ）において、点Ｐの座標と点Ｑの座標とが異な

る体に属するようにペアリングの計算を拡張することができる。また、点Ｐの座標を小さな体で定義するとペアリングの計算を高速に行うことができる。

【０１１０】

楕円曲線の定義体を変更する利点は、確実に共通鍵が１とならないようにできるという点、及び、高速に計算できるという点である。楕円曲線の定義体を変更する場合、つまり、２通りの定義体を用いる場合には、２通りの公開鍵への対応のさせ方が必要である。従来のＩＤ－ＮＩＫＳでは、エンティティがＩＤ情報によって決まる１通りの公開鍵と自身の秘密鍵とを用いて鍵共有を行っているが、この方式では、ＩＤ情報に基づいて、定義体が異なる同一の楕円曲線上の点へ、２通りの異なるやり方によって公開鍵を写像し、ＩＤ情報または公開鍵に基づき、一方のエンティティが何れか一方の定義体による公開鍵を使用し、他方のエンティティが他方の定義体による公開鍵を使用して、鍵共有を行う。

【０１１１】

全エンティティを２つのグループG_1，G_2に分ける。グループG_1に属するエンティティはＰを含む群の元を、グループG_2に属するエンティティはＱを含む群の元を夫々ＩＤ情報として用いることにより、グループG_1のエンティティとグループG_2のエンティティとにおいて鍵を共有することが可能である。

各エンティティが２種類のＩＤ情報を有しており、エンティティＡとエンティティＢとの各ＩＤ情報に何らかの大小関係を示すアルゴリズムを設定し、何れのエンティティがどちらのＩＤ情報を使用するかを決定することにより、鍵の共有化を行える。

各エンティティが２種類のＩＤ情報を有しており、両エンティティ間で２種類の値を計算し、その２つの計算値を足し合わせる等、同じ値になる演算を用いて共通鍵を生成する。

Ｐを含む群の元とＱを含む群の元との間の変換を適切に定め、その変換をシステム固有の公開情報として用いることにより、鍵の共有化が可能である。

【０１１２】

なお、上述した例では代数曲線として楕円曲線を用いる場合について説明したが、超楕円曲線を用いる場合にあっても、超楕円離散対数問題及びペアリングを

定義できるので、簡単に拡張することができる。

【０１１３】

図３は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するプログラムは、各エンティティのＩＤ情報とセンタ固有の秘密情報とに基づき前述した手法にて各エンティティ固有の秘密鍵を生成する処理（エンティティのＩＤ情報に基づき楕円曲線上の点に写像して写像値を得るステップと、その写像値とセンタ固有の秘密情報とを用いて秘密鍵を生成するステップ）を含むか、または、エンティティ自身の秘密鍵と通信相手のエンティティの公開鍵とに基づき前述した手法にて共通鍵を生成する処理（通信相手のエンティティのＩＤ情報に基づき楕円曲線上の点に写像して写像値を得るステップと、その写像値とエンティティ自身の秘密鍵とを用いて共通鍵を生成するステップ）を含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ４０は、センタ１側か、または、各エンティティ側に設けられている。

【０１１４】

図３において、コンピュータ４０とオンライン接続する記録媒体４１は、コンピュータ４０の設置場所から隔たって設置される例えばWWW(World Wide Web)のサーバコンピュータを用いてなり、記録媒体４１には前述の如きプログラム４１ａが記録されている。記録媒体４１から読み出されたプログラム４１ａがコンピュータ４０を制御することにより、各エンティティ固有の秘密鍵を生成するか、または、両エンティティ間の共通鍵を生成する。

【０１１５】

コンピュータ４０の内部に設けられた記録媒体４２は、内蔵設置される例えばハードディスクドライブまたはＲＯＭ等を用いてなり、記録媒体４２には前述の如きプログラム４２ａが記録されている。記録媒体４２から読み出されたプログラム４２ａがコンピュータ４０を制御することにより、各エンティティ固有の秘密鍵を生成するか、または、両エンティティ間の共通鍵を生成する。

【０１１６】

コンピュータ４０に設けられたディスクドライブ４０ａに装填して使用される記録媒体４３は、運搬可能な例えば光磁気ディスク，ＣＤ－ＲＯＭまたはフレキ

シブルディスク等を用いてなり、記録媒体４３には前述の如きプログラム４３ａが記録されている。記録媒体４３から読み出されたプログラム４３ａがコンピュータ４０を制御することにより、各エンティティ固有の秘密鍵を生成するか、または、両エンティティ間の共通鍵を生成する。

【０１１７】

【発明の効果】

以上詳述したように、本発明では、各エンティティのＩＤ情報から生成する公開鍵を楕円曲線上で写像するようにしたので、予備通信を行うことなく両エンティティ間で容易に共通鍵を共有し合うことができる。また、本発明ではその安全性が代数曲線上の離散対数問題に置かれており、結託攻撃などの攻撃に対して強く、ＩＤ－ＮＩＫＳの発展に本発明は寄与できる。

【図面の簡単な説明】

【図１】

本発明の暗号通信システムの構成を示す模式図である。

【図２】

２人のエンティティ間における情報の通信状態を示す模式図である。

【図３】

記録媒体の実施の形態の構成を示す図である。

【図４】

ＩＤ－ＮＩＫＳのシステムの原理構成図である。

【符号の説明】

１　センタ

１１，２１　公開鍵生成器

１２，２２　共通鍵生成器

１３　暗号化器

２３　復号器

３０　通信路

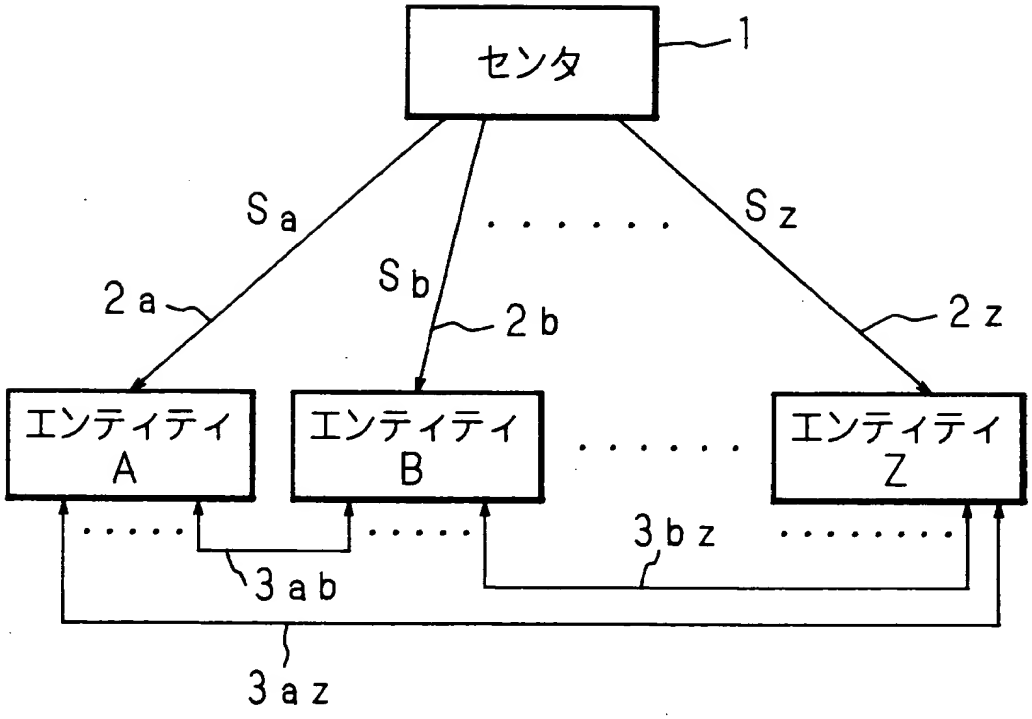
４０　コンピュータ

４１，４２，４３　記録媒体

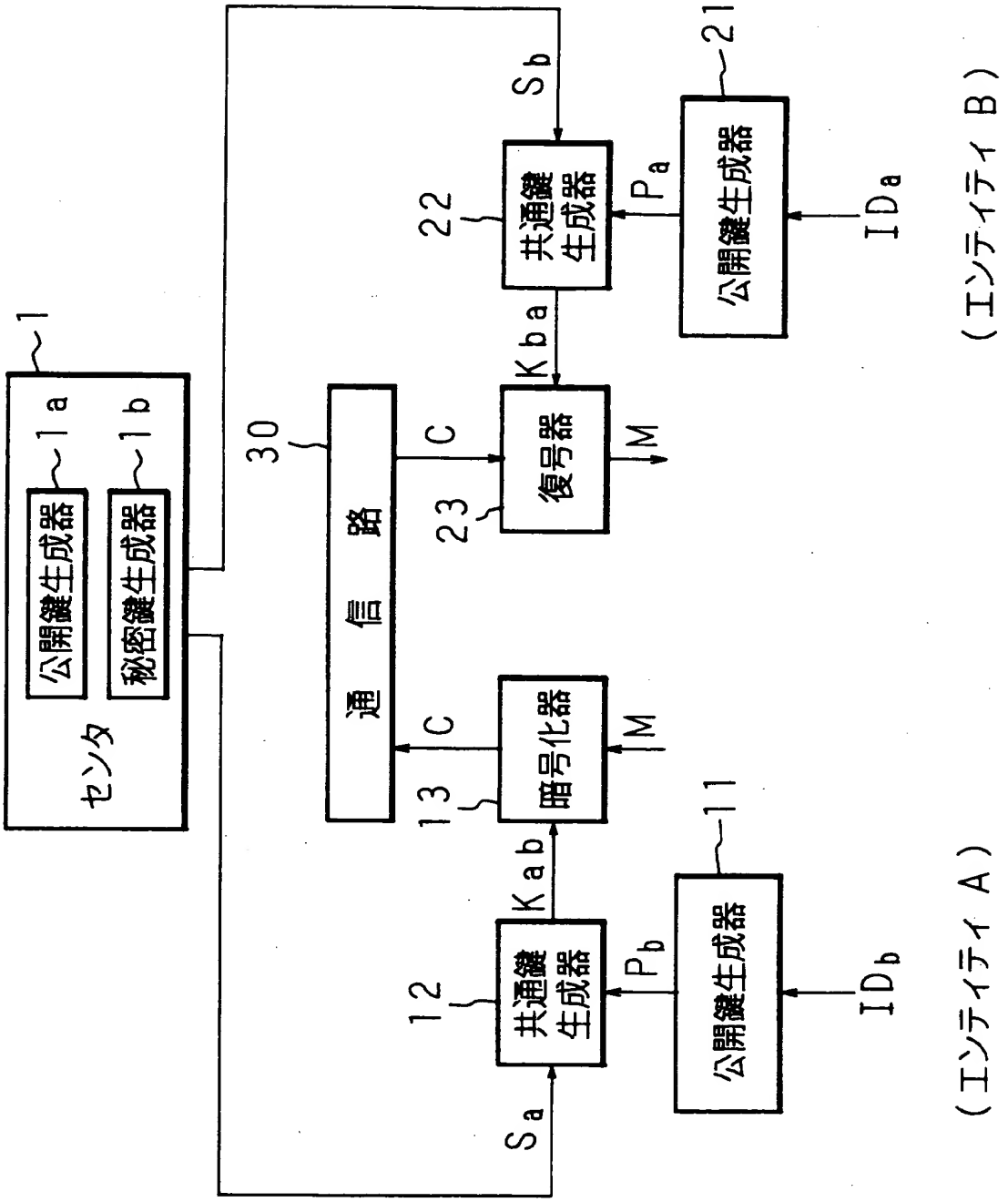
A，B，Z　エンティティ

【書類名】　　図面

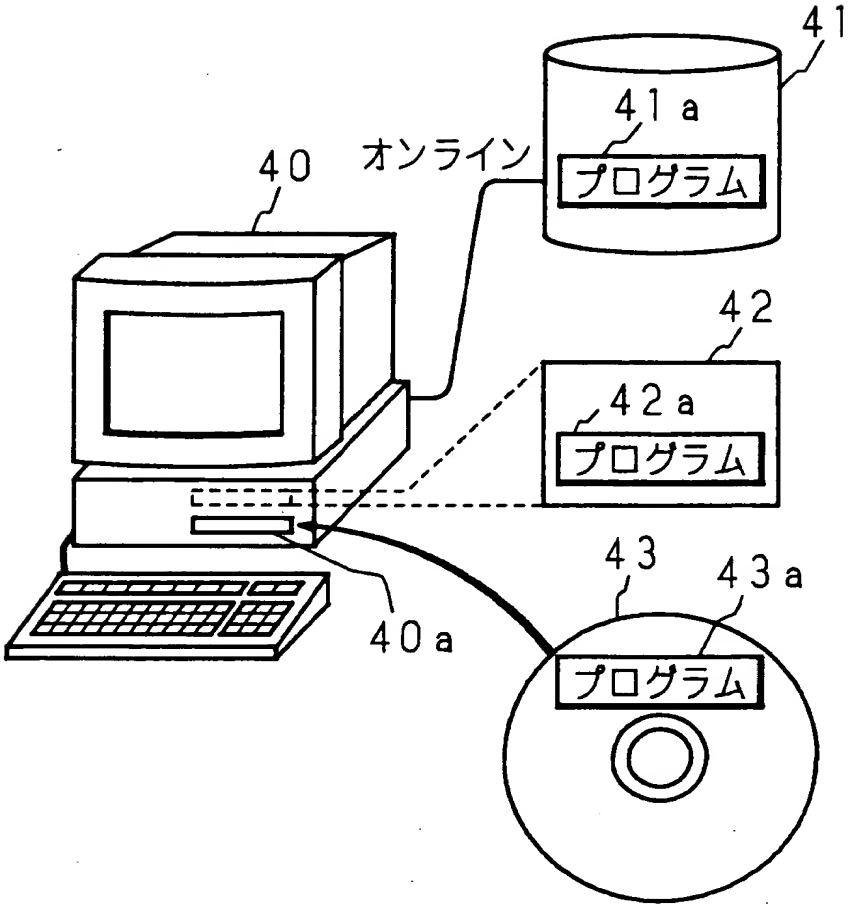
【図１】



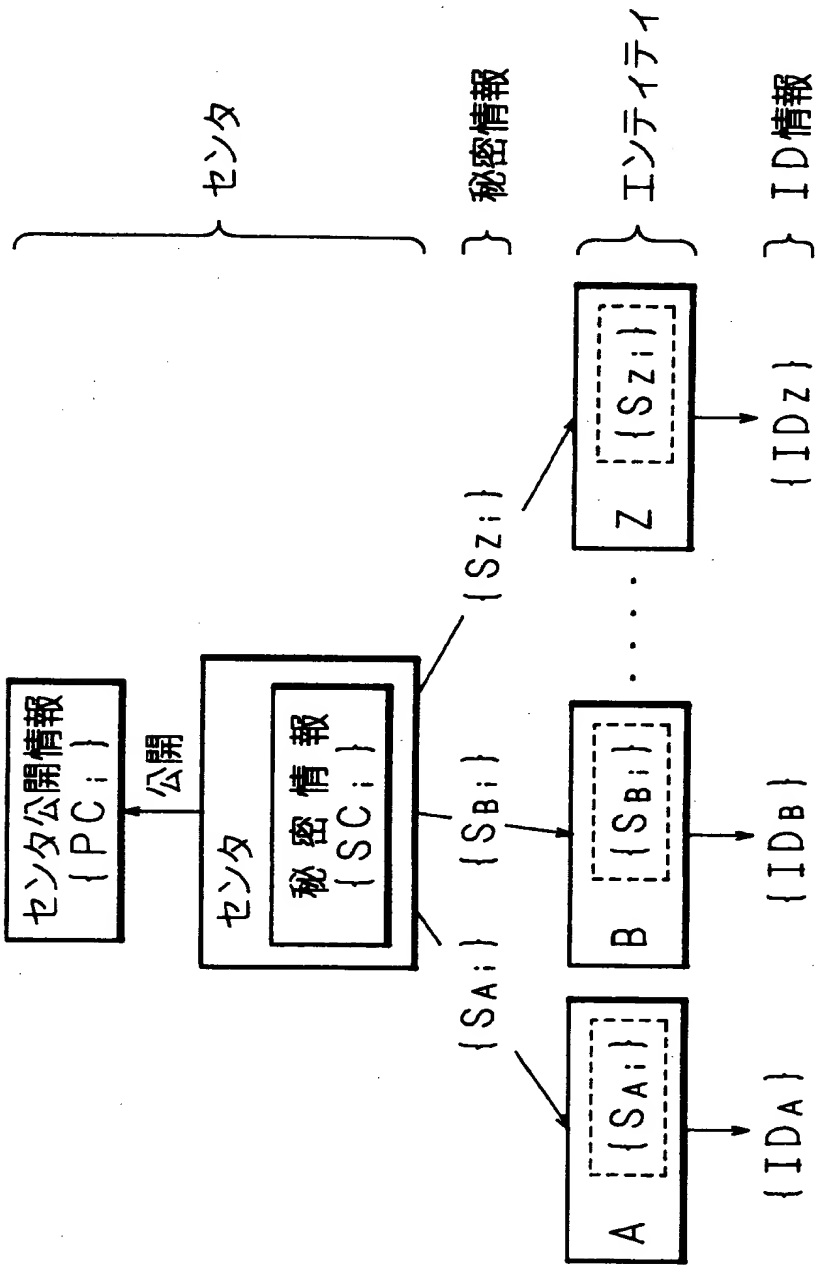
【図２】


センタ
1
1a
公開鍵生成器
1b
秘密鍵生成器
30
通信路
C
13
暗号化器
M
Kab
12
共通鍵生成器
Pb
11
公開鍵生成器
IDb
Sa
（エンティティ A）
Sb
22
共通鍵生成器
Pa
21
公開鍵生成器
IDa
（エンティティ B）
Kba
C
23
復号器
M

【図３】



【図４】


センタ
秘密情報
エンティティ
ID情報
センタ公開情報
{PCi}
公開
センタ
秘密情報
{SCi}
{Szi}
{SBi}
{SAi}
Z
{Szi}
B
{SBi}
A
{SAi}
{IDz}
{IDB}
{IDA}

【書類名】　　要約書

【要約】

【課題】　両エンティティ間で予備通信を行うことなく容易に共通鍵を共有し合える鍵共有方法、この鍵共有方法に基づいて安全なＩＤ－ＮＩＫＳを構築できる暗号通信方法及びシステムを提供する。

【解決手段】　センタ１は、各エンティティのＩＤ情報に基づき楕円曲線上の点に写像し、その写像値である公開鍵とセンタ１自身の秘密情報とを用いて、各エンティティの秘密鍵を生成する。各エンティティは、センタ１から送られる自身の秘密鍵と、通信相手のＩＤ情報に基づき楕円曲線上の点に写像した写像値である公開鍵とを用いて、暗号化処理・復号処理に用いる共通鍵を生成する。この際、楕円曲線上のペアリングを利用する。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２０００－１３３４７１
受付番号	５００００５５８７６９
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１２年　７月　７日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】　000006297
- 【住所又は居所】　京都府京都市南区吉祥院南落合町３番地
- 【氏名又は名称】　村田機械株式会社

【特許出願人】
- 【識別番号】　599100556
- 【住所又は居所】　京都府京都市山科区安朱東海道町１６－２
- 【氏名又は名称】　境　隆一

【特許出願人】
- 【識別番号】　597008636
- 【住所又は居所】　大阪府箕面市粟生外院４丁目１５番３号
- 【氏名又は名称】　笠原　正雄

【代理人】　申請人
- 【識別番号】　100078868
- 【住所又は居所】　大阪府大阪市中央区釣鐘町二丁目４番３号　河野特許事務所
- 【氏名又は名称】　河野　登夫

【選任した復代理人】
- 【識別番号】　100114557
- 【住所又は居所】　大阪府大阪市中央区釣鐘町二丁目４番３号　河野特許事務所
- 【氏名又は名称】　河野　英仁

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００６２９７〕

１．変更年月日　　１９９０年　８月　７日
［変更理由］　新規登録
住　所　京都府京都市南区吉祥院南落合町３番地
氏　名　村田機械株式会社

出　願　人　履　歴　情　報

識別番号　　〔５９９１００５５６〕

１．変更年月日　　１９９９年　７月１６日
［変更理由］　新規登録
住　所　京都府京都市山科区四ノ宮柳山町８
氏　名　境　隆一

２．変更年月日　　２０００年　６月１４日
［変更理由］　住所変更
住　所　京都府京都市山科区安朱東海道町１６－２
氏　名　境　隆一

出　願　人　履　歴　情　報

識別番号　　〔５９７００８６３６〕

１．変更年月日　　１９９７年　１月２１日
［変更理由］　新規登録
住　所　　大阪府箕面市粟生外院４丁目１５番３号
氏　名　　笠原　正雄

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.